Claims

WHAT IS CLAIMED IS:

1. A method for managing Virtual Private Network (VPN) communications, comprising:

receiving a communication from a local client which is directed to a remote client over an insecure network;

identifying a VPN associated with the communication;

translating the communication for delivery within the VPN; and

sending the translated communication via the VPN to a remote transparent VPN service, which manages VPN traffic for the remote client.

2. The method of claim 1 further comprising, processing the method as a local transparent VPN service, which manages VPN traffic for the local client.

3. The method of claim 1 wherein receiving further comprising, directing the communication from the local client to the method based on the local client attempting to access a defined port, the defined port is associated with a switch or router that relays the communication to the method.

4. The method of claim 1 further comprising, interacting with the remote transparent VPN service to manage additional communications between the local client and the remote client via the VPN.

5. The method of claim 4 further comprising, caching data received from the remote transparent VPN service in a local cache for accelerated delivery to the local client.

6. The method of claim 1 wherein receiving the communication further includes receiving the communication in at least one of a File Transfer Protocol

(FTP) format and a Transmission Control Protocol (TCP) format.

7. The method of claim 1 further comprising, communicating with the remote transparent VPN service over the insecure network via Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

8. A method for managing Virtual Private Network (VPN) communications, comprising:

receiving a communication from a local client which is directed to a remote client associated with a VPN; and

inspecting the communication for determining whether the communication is a request for data that resides in a local cache, and if so, delivering the data to the local client, and if not, locating a remote transparent VPN service associated with the VPN, and wherein the communication is translated into formats used by the VPN and sent securely over an insecure network to the remote transparent VPN service for delivery to the remote client.

9. The method of claim 8 wherein inspecting further includes establishing secure communications with the remote transparent VPN service using at least one of Sockets Layer(SSL) and Transport Layer Security (TLS).

10. The method of claim 8 wherein inspecting further includes identifying the remote transparent VPN service as a service which is managing VPN traffic for the remote client.

11. The method of claim 8 wherein receiving further includes intercepting the communication issued from the local client by using a router or switch, wherein the local client directs the communication to the remote client via the communication port and the router or switch relays the communication to the processing of the method.

12. The method of claim 8 further comprising:

receiving a response communication from the remote client via the remote transparent VPN service, if the communication had been sent via the VPN because it could not be satisfied from the local cache;

translating the response based on the formats of the VPN; and

delivering the translated response to the local client.

13. The method of claim 8 further comprising, managing additional communications associated with the VPN from one or more different local clients which are directed between one or more different remote clients, wherein the remote transparent VPN service manages the additional communications on behalf of the one or more different remote clients.

14. The method of claim 8 wherein receiving further includes intercepting the communication after detecting that the local client is transmitting the communication with a non-Hypertext Transfer Protocol (HTTP).

15. The method of claim 8 further comprising, interacting with the remote transparent VPN service with mutually signed certificates that are exchanged between the method and the remote transparent VPN service during the interactions.

16. A Virtual Private Network (VPN) managing system, comprising:

a remote transparent VPN service; and

a local transparent VPN service, wherein local transparent VPN service intercepts and manages VPN traffic on behalf of one or more local clients and services communications of those local clients with data in a local cache, if available, and if the data is not available in the local cache, the local transparent VPN service transmits the communications securely to the remote transparent VPN service for delivery and servicing by one or more remote clients which the remote transparent VPN service manages.

17. The VPN managing system of claim 16 wherein the local transparent VPN service and the remote transparent VPN service interact via at least one of Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

18. The VPN managing system of claim 16 wherein the local transparent VPN service intercepts local VPN traffic on behalf of the one or more local clients by inspecting Transmission Control Protocol (TCP) or File Transfer Protocol (FTP) communications originating from the one or more local clients.

19. The VPN managing system of claim 16 wherein the local transparent VPN service intercepts the VPN traffic through a router or switch which is configured to relay communications on a defined port to the local transparent VPN service.

20. The VPN managing system of claim 16 wherein communications between the local and remote transparent VPN services occur with mutually exchanged certificates.

21. A Virtual Private Network (VPN) managing system, comprising:

a communication port; and

a local transparent VPN service, wherein VPN communications directed to the communication port are relayed to the local transparent VPN service, the local transparent VPN service attempts to service the VPN communications from local cache and if attempts fail, the local transparent VPN service securely communicates with a remote transparent VPN service via an insecure network to service the VPN communications.

22. The VPN managing system of claim 21 further comprising a router or switch which relays the VPN communications to the local transparent VPN service.

23. The VPN managing system of claim 21, wherein the system resides on a server and services a plurality of local clients associated with the VPN

communications.

24. The VPN managing system of claim 21 wherein the system resides on a single client.

25. The VPN managing system of claim 21 wherein the local transparent VPN service translates and services the VPN communications on behalf of a one or more of local clients.

26. The VPN managing system of claim 25 wherein the remote transparent VPN service translates and service the VPN communication on behalf of a one or more of remote clients.